

EXHIBIT 6

USAO 000494

~~(b) (5) DPP~~

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<div style="text-align: center;"> _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> _____ <i>Printed name and title</i> </div>	

Copy of warrant and inventory left with:

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on March 9, 2018, and currently maintained in the custody of the Federal Bureau of Investigation, in Los Angeles, California:

1. Black LG Android cell phone, Model Number LGLS991, IMEI Number 357355062960973, with cord (hereinafter "SUBJECT DEVICE 1");
2. Silver Samsung cell phone with broken screen, Model Number SM-J327P (hereinafter "SUBJECT DEVICE 2"); and
3. Gold LG Cell Phone with broken screen, Model Number LS990, Serial Number 410KPVH0351583 (hereinafter "SUBJECT DEVICE 3," and collectively, the "SUBJECT DEVICES").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a) (2) (Receipt and Distribution of Child Pornography) and 2252A(a) (5)(B) (Possession of Child Pornography) (collectively, the "Subject Offenses"), namely:

- a. Child pornography, as defined in 18 U.S.C. § 2256(8).
- b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to, documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.
- c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256(8).
- d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages,

that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(B).

e. Any records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to peer-to-peer file-sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the SUBJECT DEVICES.

i. Any SUBJECT DEVICE used to facilitate the above-listed violations (and forensic copies thereof).

j. With respect to any SUBJECT DEVICE used to facilitate the above-listed violations or containing evidence

falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

2. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return

the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

3. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to

law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Benjamin G. Cook, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant for the following digital devices currently in the custody of the Federal Bureau of Investigation, in Los Angeles, California, as described more fully in Attachment A:

a. Black LG Android cell phone, Model Number LGLS991, IMEI Number 357355062960973, with cord (hereinafter "SUBJECT DEVICE 1");

b. Silver Samsung cell phone with broken screen, Model Number SM-J327P (hereinafter "SUBJECT DEVICE 2"); and

c. Gold LG Cell Phone with broken screen, Model Number LS990, Serial Number 410KPVH0351583 (hereinafter "SUBJECT DEVICE 3," and collectively, the "SUBJECT DEVICES").

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2) (Receipt and Distribution of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there

is sufficient probable cause for the requested search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since June 2012. I am currently assigned to a Violent Crimes Against Children squad in the Los Angeles Field Office. In that capacity, I investigate the sexual exploitation of children and child pornography, including violations of 18 U.S.C. § 2252(a) and § 2252A, in the Central District of California, as part of the Southern California Regional Sexual Assault Felony Enforcement Team. During my tenure as a Special Agent, I have executed and participated in the execution of numerous search and arrest warrants and seized evidence of violations of United States law.

5. I gained expertise in child exploitation investigations through formal training and on-the-job training with more experienced agents and received training and experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, surveillance, and a variety of other investigative tools available to law enforcement officers. In addition, I received specialized training in the sexual exploitation of children, observed and reviewed images of child pornography in many forms of media, including computer and digital media and participated in

numerous interviews and debriefings of persons involved in the sexual exploitation of children. I have conducted and participated in numerous investigations related to the sexual exploitation of children which have resulted in the arrest and conviction of individuals.

6. Through my training and experience, I have become familiar with methods used by people who commit offenses involving the sexual exploitation of children. My training and experience has given me an understanding of how people who commit offenses related to the sexual exploitation of children use digital devices and the Internet to facilitate and commit those offenses.

III. SUMMARY OF PROBABLE CAUSE

7. On March 5, 2018, as part of a child pornography investigation, the FBI served a residential search warrant and seized 18 digital devices requiring forensic review. The FBI has completed its review of 15 of those devices and seeks this warrant for additional time to search the remaining three SUBJECT DEVICES.

IV. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

8. Based the facts set forth above, and my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, there is probable cause to believe that the user of the SUBJECT DEVICES has a sexual interest in children and images of children. Based upon my knowledge, experience, and training in child pornography

investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in-person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess hard copies of child pornography, such as pictures, films, video tapes, magazines, negatives, photographs, etcetera. As digital technology has developed, individuals with a sexual interest in children or images of children have become much more likely to

maintain child pornography in digital or electronic format, stored either on digital devices, or in remote storage locations on the Internet. Regardless of whether these individuals collect their child pornography in hard copy or digital format, they may maintain their child pornography for a long period of time, even years. They usually maintain these collections in a safe, secure, and private environment, such as their homes, vehicles, or nearby, so they can view the child pornography at their leisure. These collections are typically highly valued.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; may conceal such correspondence as they do their sexually explicit material; and may often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children typically prefer not to be without child pornography for prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Based on my training and experience, as well as my conversations with digital forensics agents, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via computer. Electronic files downloaded to

a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Because computer evidence is recoverable after long periods of time, there is probable cause to believe that evidence of activity related to the receipt, possession and distribution of child pornography will be found on the SUBJECT DEVICES.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

9. As used herein, the term "digital device" includes the SUBJECT DEVICES.

10. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

11. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

12. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. STATEMENT OF PROBABLE CAUSE

13. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Background of the Investigation

14. On August 12, 2017, an unknown individual using the mobile messaging application "Kik" sent an FBI Online Covert Employee ("OCE") a link to a Dropbox account containing approximately 42 files of suspected child pornography. On the same date, the same individual told the FBI OCE that he had previously had sex with a five year old and a seven year old. The IP address from which the link containing child pornography was sent was subscribed to a residence located at 3052 W. Cherylllyn Lane, Anaheim, CA 92804 (the "SUBJECT PREMISES").

15. On or about March 5, 2018, in case number 18-MJ-00484, the Honorable Rozella A. Oliver, United States Magistrate Judge,

signed a warrant authorizing the search of the property located at the SUBJECT PREMISES, as well as the seizure of digital devices from the SUBJECT PREMISES and a search of those devices for evidence of the Subject Offenses for a period of 120 days. The signed warrant application is attached hereto as Exhibit 1 and incorporated herein by reference.

B. Search Warrant Execution

16. On or about March 9, 2018, federal agents executed the warrant at the SUBJECT PREMISES and seized a number of digital devices ("the Seized Digital Devices"), which included the SUBJECT DEVICES. Based on the terms of the original search warrant, the government had until July 7, 2018, to retain and search the Seized Digital Devices.

C. Status of the Digital Devices Search

17. The FBI began its review of the Seized Digital Devices shortly after the execution of the search warrant. Certain devices proved more difficult to examine. On or about March 22, 2018, the FBI delivered SUBJECT DEVICE 2 and SUBJECT DEVICE 3 to forensic specialists from the Los Angeles County Sheriff's Department, High Tech Task Force in order to decrypt them. Following decryption, SUBJECT DEVICE 2 and SUBJECT DEVICE 3 were taken to the Orange County Regional Computer Forensics Lab ("OCRCFL") for forensic imaging. During this process, forensic specialists discovered numerous images of child pornography on SUBJECT DEVICE 3, including the following:

a. An image file entitled "1024_x768_bestfit.jpg" shows the torso and legs of a nude prepubescent female. The

prepubescent female has her legs spread exposing her vagina. An adult male is anally penetrating the female with his erect penis.

b. An image file entitled "large.jpg" depicts a nude prepubescent female lying on her back. The female's legs are spread and raised in the air, bent at the knees. The female's vagina and anus are exposed.

18. The government completed its review of 12 of the 18 Seized Digital Devices by the time the original search warrant expired on July 7, 2018. At this time the government halted its search of the Seized Digital Devices. On October 9, 2018, the Honorable Karen L. Stevenson, United States Magistrate Judge, signed a first search warrant extension order, nunc pro tunc, authorizing the continued search of the six remaining Seized Digital Devices, which included the SUBJECT DEVICES, until December 9, 2018. A copy of this first extension application and order is attached hereto as Exhibit 2 and incorporated by reference.

19. On November 19, 2018, the FBI took custody of SUBJECT DEVICE 3, following OCRCFL's completion of the forensic imaging for that device.

20. On December 10, 2018, the Honorable Paul L. Abrams signed a second search warrant extension order authorizing the continued search of the SUBJECT DEVICES for an additional 60 days, until March 10, 2019. A copy of this second extension application and order is attached hereto as Exhibit 3 and incorporated by reference.

21. On January 22, 2019, the FBI took custody of SUBJECT DEVICE 3, following OCRCFL's completion of the forensic imaging for that device.

22. On March 7, 2019, the Honorable Paul L. Abrams signed a third search warrant extension order authorizing the continued search of the SUBJECT DEVICES for an additional 90 days, until June 5, 2019. A copy of this third extension application and order is attached hereto as Exhibit 4 and incorporated by reference. Upon expiration of the authorized search period, law enforcement stopped searching the SUBJECT DEVICES.

D. FBI Needs Additional Time to Search the SUBJECT DEVICES

23. Additional time is necessary to complete the review of the contents of the SUBJECT DEVICES and "bookmark" only the information allowed under the legal authority provided in the search warrant.

24. I took over as the case agent for this investigation in March 2019, after the departure of the prior case agent. Although by that time the forensic images of the SUBJECT DEVICES were created, due to my heavy caseload of active child exploitation investigations that predate this case, I was unable to complete my review of the SUBJECT DEVICES and write the necessary forensic reports before expiration of the third extension.

25. The forensic review of digital devices is time consuming. Agents cannot simply turn on computers and review their contents because merely turning on a computer and

reviewing its contents changes the data on the computer. Specialized computer software is therefore needed to ensure that evidence remains in a pristine and usable condition, and is not affected by the review process. The review also must be conducted by agents who have received specialized training to ensure that the review is done thoroughly and in a forensically sound fashion. This process takes substantial time.

26. The SUBJECT DEVICES alone contain approximately 90 gigabytes of data. The information stored on the cell phones hold an unknown amount of storage, but smart phones can hold several Gigabytes of information, as well as several Gigabytes of deleted information which agents will have to review. Processing and reviewing all these devices and documenting them is time consuming.

27. Further, the number of digital devices, the amount of time for the computer systems to read the data for viewing, and for the investigator to view and "bookmark," or label, the images of contraband as evidence are tasks which require a significant amount of time.

///

///

///

VII. CONCLUSION

28. For all of the reasons described above, there is probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES described in Attachment A.

/S/

Benjamin G. Cook, Special
Agent, Federal Bureau of
Investigation

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 21 day of
April, 2020



HON. GAIL STANDISH
UNITED STATES MAGISTRATE JUDGE